Abstract of **CN1414759**

A system of controlled multicast includes an Ethernet exchanger, a multicast router 2,a protal server 3 and a AAA server 4 being connected with the said multicast router, which down-going of Ethernetexchanger is connected with the client host computer and upgoing of it is connected with the multicast router 5 which completes the double layer of multicase exchange, the portal server 3 is used as an authentication interface of the client and the AAA server 4 is used to keep the authority configuration of entering multicast for the client, the up-going of multicast router 2 which connects to the multicast router 5 in the other system cooperates with AAA server 4 to finalize the authority authentication of entering multicast for the client together and to issue to control command based on the authentication result to control the Ethernet to carry on the multicast retransmission.

[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 29/06

[12] 发明专利申请公开说明书

[21] 申请号 02100445.5

[43] 公开日 2003 年 4 月 30 日

[11] 公开号 CN 1414759A

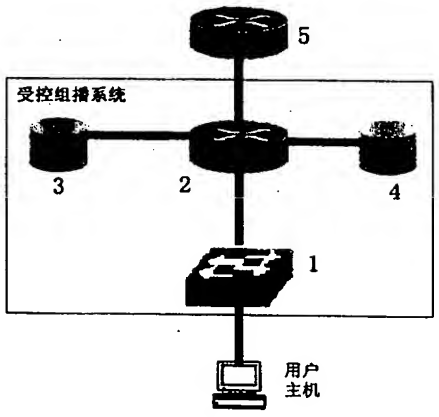
[22] 申请日 2002.1.30 [21] 申请号 02100445.5
[71] 申请人 华为技术有限公司
地址 518057 广东省深圳市科技园科发路华为用服大厦
[72] 发明人 周 鹏 刘 越 钟 凯 阳光贤 刘克彬 彭昆成

[74] 专利代理机构 北京德琦专利代理有限公司
代理人 夏宪富
权利要求书 4 页 说明书 13 页 附图 5 页

[54] 发明名称 受控组播的系统及其实现方法

[57] 摘要

一种受控组播的系统及其实现方法，该系统包括：以太网交换机 1、组播路由器 2，以及与该组播路由器相连接的 portal 服务器 3 和 AAA 服务器 4，其中以太网交换机 1 下行连接各用户主机，上行与组播路由器 5 相连接，其完成二层组播交换；portal 服务器 3 用作用户接入认证的接口，AAA 服务器 4 用于保存用户加入组播组的权限配置；组播路由器 2 上行连接其他系统的组播路由器 5，配合 AAA 服务器 4 一起共同完成对用户加入组播组的权限认证，并按照认证的结果下发控制命令，控制以太网交换机 1 进行组播转发。 本发明的实现方法较好地解决对参与组播的发送者与接收者的授权认证和受控加入问题，能方便地识别加入或离开组播组的用户，可通过用户下线主动停止用户的组成员身份；且不影响转发效率。



ISSN1008-4274

知识产权出版社出版

1、一种受控组播的系统，包括有以太网交换机和组播路由器，其中以太网交换机下行连接各用户主机，上行与组播路由器相连接，该组播路由器上行连接其他系统的组播路由器，该以太网交换机完成二层组播交换，该以太网交换机与用户主机之间使用 IGMP V2 协议作为组管理协议；其特征在于：该受控组播系统还包括有：与该组播路由器相连接的 portal 服务器和 AAA 服务器，其中 portal 服务器用作用户接入认证的接口，AAA 服务器用于保存用户加入组播组的权限配置，例如在 AAA 服务器上配置有每个用户有权加入的每个组播组的地址等；该组播路由器则配合 AAA 服务器一起共同完成对用户加入组播组的权限认证，并按照认证的结果下发控制命令，控制以太网交换机进行组播转发。

2、根据权利要求 1 所述的受控组播的系统，其特征在于：所述的组播路由器与 AAA 服务器之间采用对标准 AAA 协议扩展了的华为公司的 radius+协议作为通信协议，而以太网交换机和组播路由器之间采用华为公司的华为组管理协议 HGMP（Huawei Group Management Protocol）作为控制协议。

3、一种受控组播的实现方法，其特征在于：该方法包括有下列步骤：首先进行接入认证处理，再由以太网交换机按端口划分vlan及对主机IGMP报文进行处理，以及进行用户的识别、加入组播的认证及由路由器对IGMP报文进行处理，接着由组播路由器控制以太网交换机进行组播转发，两者之间采用HGMP协议作为受控组播的控制协议；之后，交换机对HGMP控制报文进行处理和进行组播流的转发；主机完成转发后，就退出组播组并作相应的处理。

4、根据权利要求3所述的受控组播的实现方法，其特征在于：该方法的具体操作步骤是：

（1）首先进行接入认证处理：当一主机访问网络时，首先要通过portal服务器提供的接口输入包括有用户名和密码的认证信息，并由AAA服务器通过这

些信息来认证该主机的身份；通过认证后，路由器将该主机的用户标识及其对应的vlan号记录在一个“用户组播访问权限表”中；

（2）以太网交换机按端口划分vlan及对主机IGMP报文进行处理：以太网交换机是根据端口划分vlan，每个端口划分为一个vlan，且其每个端口连接一个主机用户，当交换机收到主机发来的IGMP报文时，用该报文的目的MAC地址查找CAM表进行转发，其转发流程与单播报文相同：即若查到该目的MAC地址所对应的端口时，按查到的端口转发组播报文，若没有查到该目的MAC地址所对应的端口时，将组播报文转发到所有端口；

（3）进行用户的识别、加入组播的认证及路由器对IGMP报文进行处理：路由器收到IGMP Membership Report报文后，因为组播路由器收到的从以太网交换机发来的数据包都有vlan号，通过查找第（1）步骤中记录的“用户组播访问权限表”，可以知道对应用户的UserID，也就是知道该IGMP Membership Report报文是哪个用户发送的，然后以查到的UserID为用户名，以主机所要加入的组播地址为属性，发送扩展的radius认证报文到AAA服务器进行认证，由AAA服务器根据用户申请的业务决定是否让用户加入：如果用户拥有权限，则发送accept报文作回应，否则发送reject报文回应；路由器收到reject报文后不作任何处理，收到accept报文后将用户能够加入的组的组播地址写到“用户组播访问权限表”中，并对该主机加入的报文作通常组播路由器的例行处理，然后生成一个HGMP Join报文发送到交换机，该报文包含了申请加入组播组的主机所连接的端口对应的vlan号和申请加入的组播地址，并且包含Join命令域；此外，组播路由器还要如同普通组播路由器一样地对IGMP Membership Report报文进行建立组播转发树的常规处理；

（4）由组播路由器控制以太网交换机进行组播转发，两者之间采用HGMP协议作为受控组播的控制协议：在以太网交换机上由组播路由器控制其组播转发表的生成与删除，当组播路由器允许某个主机加入某个组时，它给交换机发送包含有申请加入组播组的主机的vlan号和申请加入的组播地址的HGMP join

报文；当组播路由器要终止某个主机加入某个组时，它给交换机发送包含有终止加入组播组的主机的vlan号和终止加入的组播组地址的HGMP leave报文，通过这种方法，组播路由器控制以太网交换机的的组播转发；

（5）交换机对HGMP控制报文进行处理：当交换机收到HGMP Join报文后，用组播地址对应的mac地址查CAM表，如果能够找到与其对应的一个表项，则通过报文中的vlanID查表来获得该主机端口号，然后将该端口号加入到该表项中；如果不能找到，则在CAM表中增加一个表项，该表项包含该组播地址所对应的mac地址、申请加入组播组的主机的端口号以及与交换机相连的路由器的端口号；当交换机收到HGMP Leave报文后，用组播地址对应的mac地址查CAM表而得到一个表项，再通过vlanID查表来获得该主机端口号，然后将该端口号从该表项中删除，如果该端口号是该表项的唯一一个端口，则删除整个表项；

（6）组播流的转发：当路由器收到组播源发来的组播流时，将该组播流按照转发表转发给出端口，路由器在处理主机的IGMP Membership Report报文时，不是按vlan号而是按交换机的实际端口建立组播转发出口，所以一个连接路由器的交换机在组播转发表中只有一个出口，组播流只发一份拷贝到交换机；

（7）主机退出组播组：当主机完成组播后，需要退出组播组时，由主机发送IGMP Leave报文要求退出组播组，路由器在收到该离开报文后，提取报文中的vlanID，并通过它查找第（1）步骤中建立的“用户组播访问权限表”得到对应的表项，删除该表项中成员离开报文所指示的组播地址，并完成通常路由器对成员离开报文的例行处理，再生成一个HGMP Leave报文发给交换机，该报文包含了想要离开组播组的主机的vlan号和要离开的组播地址，并且包含Leave命令域。

5、根据权利要求 3 所述的受控组播的实现方法，其特征在于：所述的以太网交换机的组播转发表与单播转发表是共用的。

6、根据权利要求 3 所述的受控组播的实现方法，其特征在于：以太网交换机在转发报文时，若报文转发到组播路由器端口，使用 vlan 协议；否则，向别

的端口发送报文时不用 vlan 协议。

7、根据权利要求 3 所述的受控组播的实现方法，其特征在于：上述第（6）步骤中的组播路由器发送给交换机的组播数据包不加 vlan 号，以避免为同一个交换机上的不同主机的每个 vlan 分别发送一份数据而浪费带宽的缺陷。

8、根据权利要求 3 所述的受控组播的实现方法，其特征在于：上述第（7）步骤中的主机退出组播组的操作还可以通过下述方法实现之：路由器在获知用户下线时主动发送 HGMP Leave 报文而停止向用户发送组播流，其具体实现方法与 IGMP Leave 报文的操作步骤相同。

9、根据权利要求 3 所述的受控组播的实现方法，其特征在于：该受控组播的实现方法还对组播发送者进行控制：当主机向某个组播组发送数据时，第一个接收该数据的组播路由器利用组播访问控制列表（Access Control List，简称：ACL）对数据报文进行过滤，只有满足其要求的报文才能被转发到组播树。

10、根据权利要求 9 所述的受控组播的实现方法，其特征在于：所述的组播访问控制列表 ACL 是由命令字、源地址和组地址（即：目的地址）构成。

11、根据权利要求 9 所述的受控组播的实现方法，其特征在于：所述的组播访问控制列表 ACL 是由一个集中的组播业务控制服务器来下发给各组播路由器，以便路由器藉由该组播访问控制列表 ACL 完成控制发送者的功能，该组播业务控制服务器同时兼作 AAA 服务器。

12、根据权利要求 9 或 11 所述的受控组播的实现方法，其特征在于：所述的组播访问控制列表 ACL 也可通过一个集中的策略服务器或网管下发，以消除分散配置引起的不便。

受控组播的系统及其实现方法

所属领域

本发明涉及一种IP组播技术，确切地说，涉及一种IP受控组播的系统及其实现方法，属于通信技术领域。

背景技术

随着IP组播技术的成熟，IP组播应用越来越多，但是在IP模型中，任何一台主机都能够不受限制地加入到任何一个组播组，到目前为止，还没有一种方法能够有效解决IP组播网中的主机受控加入问题。

众所周知，在IP组播模型中，一个组播组是由发送者和接收者组成的，发送者到接收者之间由组播分布树连接。当发送者需要向某个组发送数据时，主机直接把数据发送到与其相连的路由器，该路由器将该数据通过组播分发树转发给组播接收者，路由器不对发送报文的主机作任何限制。当一台主机想接收某个组播组的数据时，它根据因特网组管理协议（Internet Group Management Protocol，简称：IGMP协议）向与其相连的路由器发送Member report报文，该路由器处理此报文之后会将收到的该组播组数据转发给该主机；同样，路由器不会对想接收组播报文的主机作任何限制。随着IP组播应用的商业化，组播安全已经成为必须尽快获得解决的一个问题，而阻止未授权的接收者接收组播报文是组播安全的关键一环。

Norihiro Ishikawa等人曾提出IGMP扩展协议《IP组播授权的IGMP扩展》（IGMP Extension for Authentication of IP Multicast，刊于draft-ietf-idmr-igmp-auth-01.txt）和RADIUS扩展协议《组播路由器认证的RADIUS扩展》（RADIUS Extension for Multicast Router Authentication，其中远

程拨号用户认证服务RADIUS为Remote Authentication Dial In User Service的缩写，刊于draft-yamanouchi-radius-ext-00.txt），可以对发送者和接收者进行认证。

上述的IGMP扩展协议是在IGMP V2的基础上进行扩展，它增加了对组播发送者和接收者的认证功能，阻止未授权的用户发送/接受组播包。IGMP扩展协议使用一种需要经过三次握手、口令加密的类似PPP验证协议CHAP（Challenge Handshake Authentication Protocol）的Challenge-Response机制来认证用户。当一个组播发送者开始发送IP组播报文时，入口路由器就可以用challenge-response机制认证它。入口路由器在认证的时候可以使用RADIUS作为认证服务器。当认证通过后，该发送者发送的组播包就可以被入口路由器转发到IP组播网中到达出口路由器。当认证不成功时，入口路由器丢弃该发送者发送的组播包（silently）。当一个组播接收者想要接收IP组播报文时，通过出口路由器认证它。出口路由器在认证时可以使用RADIUS作为认证服务器。当认证通过后，出口路由器开始将IP组播包发送到该接收者。当认证不成功时，出口路由器不转发IP包到该接收者。

上述RADIUS扩展协议是在RADIUS的基础上进行扩展，它可以在入口路由器和出口路由器处对组播发送者和接收者进行认证，并跟踪用户的组播数据，为业务管理提供数据。认证服务器必须能够提供路由器请求的认证业务，认证时路由器提供user ID和口令。为了安全，认证时要求使用基于challenge的认证。还必须对每个业务进行认证，如对每个组播组地址进行认证。这是因为组播包是按组地址发送的，用户的权限应该与组相关联。除了再增加一些属性，其他方面的要求与RADIUS一样。路由器是否使用RADIUS认证是可以选择的。

当组播路由器被配置成支持使用RADIUS计费时，在组播业务的开始，它会生成一个计费开始报文，并发送到RADIUS组播计费服务器。该计费开始报文描述了业务的类型，RADIUS组播计费服务器在收到该报文后会回送一个确认报文。在组播业务结束时，组播路由器也会生成一个计费结束报文，并发送

到RADIUS组播计费服务器。该计费结束报文描述了业务的类型，RADIUS组播计费服务器在收到该报文后会回送一个确认报文。

当组播路由器收到一个IGMP-Join请求后，它发送一个Access-Request报文给RADIUS组播认证服务器请求认证。在收到从RADIUS组播认证服务器发来的认证通过响应后，组播路由器发送一个Account-Request/Start报文给RADIUS组播计费服务器开始计费。当组播路由器收到一个IGMP-Leave请求后，它发送一个Account-Request/Stop报文给组播计费服务器结束计费。如果在一定时间内组播路由器没有收到响应，RADIUS扩展协议建议组播路由器再连续重发几次Access-Request报文。组播计费服务器可以请求别的服务器来完成计费功能（proxy）。当计费服务器不能成功记录计费报文时，它不能发送Accounting-Response确认报文给组播路由器。

此外，CISCO公司开发了CISCO组管理协议（CISCO Group Management Protocol，简称：CGMP）用于解决以太网交换机环境下的组播转发泛滥（flooding）的问题，通过CGMP，三层设备可以控制二层设备的转发表，从而提供了一种手段，可以在一定程度上控制用户的授权接收。CGMP的报文格式如图1所示，是由版本号（Ver）4比特、类型（Type）4比特、保留部分（Reserved）2字节、报文中GDA/USA对的个数（Count）1字节和若干个GDA/USA对组成。其中GDA（Group Destination Address）是一个MAC组播地址，是主机所要加入的组播组的IP地址对应的MAC地址，USA（Unicast Source Address）是要加入组播组的主机的MAC地址，它是一个单播地址。

参见图2所示，CGMP方法的工作过程如下：主机Host 1发送IGMP Membership Report报文加入组播组224.1.2.3，交换机用从该报文中解析出来的组地址对应的mac地址0100.5e01.0203查找CAM表，因为CAM表中没有匹配项，该报文被转发（flooding）到包括cpu和组播路由器的所有端口。其中组播路由器收到IGMP Membership Report报文后，除了对该报文进行例行处理外，还生

成一个CGMP Join报文组播到交换机，该报文包含了申请加入组播组的主机的mac地址（USA：0080.c7a2.1093）和申请加入的组对应的mac地址（GDA：0100.5e01.0203），并且包含Join命令域。当交换机收到该CGMP Join报文后，在CAM表中加入一个表项，包含GDA（图示为：0100.5e01.0203）、申请加入组播组的主机的端口号（图示为：2）以及与交换机相连的路由器的端口号（图示为：1）。其中，主机端口号是通过USA查表获得的。

参见图3，当第四个主机Host 4加入组播组224.1.2.3时，同样发送IGMP Membership Report报文到交换机，交换机解析出加入的组为224.1.2.3，使用其对应的mac地址0100.5e01.0203查找CAM表，结果是找到该表项，并将报文发送到该表项列出的端口1和2(即路由器和Host 1)。而路由器收到IGMP Membership Report报文后，除了对该报文进行例行处理外，还生成一个CGMP Join报文组播到交换机，该报文包含了申请加入组播组的主机的mac地址（USA：0080.c7b3.2174）和申请加入的组对应的mac地址（GDA：0100.5e01.0203），并且包含Join命令域。当交换机收到该CGMP Join报文后，用GDA查找CAM表得到一个表项，通过USA查表获得主机4的端口号5，然后将该端口号5加入到该表项中。

上述的IGMP扩展协同RADIUS扩展的方法虽然解决了发送者与接收者的授权问题，但是仍然存在以下缺点：（1）在共享网络上只要有一个主机加入成功，则其他所有主机都能接收到该组播数据，因此无法对未授权主机接收组播数据的状况进行控制。如果采用密钥方法来解决此问题，则必须在认证前对各个主机分发密钥，这又会带来许多限制和麻烦。（2）如果采用该两个协议，不但要更新路由器设备，还需要修改主机侧的IGMP软件。而且，这两个协议都还没有标准化，目前的主机都不支持IGMP扩展。而CISCO公司的CGMP方法的缺点是：（1）没有将路由器对二层交换机的转发控制与主机/用户的授权接收联系起来，只是提供了控制二层交换机组播报文在其端口泛滥的控制方法，也没

有提供认证授权用户加入组播组的方法。（2）路由器不能探测出主机/用户的“无声撤离”（Silent leave）。

发明内容

本发明的目的是提供一种受控组播的系统，该系统为本发明实现受控组播的方法提供了实施环境。

本发明的另一目的是提供一种受控组播的实现方法，该方法能够克服上述 IGMP 扩展与 RADIUS 扩展协同工作以及 CISCO 公司的 CGMP 这两种现有的组播方法的各种缺陷，可以较好地解决对参与组播的发送者与接收者的授权认证和受控加入的问题。

本发明的目的是这样实现的：一种受控组播的系统，包括有以太网交换机和组播路由器，其中以太网交换机下行连接各用户主机，上行与组播路由器相连接，该组播路由器上行连接其他系统的组播路由器，该以太网交换机完成二层组播交换，该以太网交换机与用户主机之间使用 IGMP V2（版本 2）协议作为组管理协议；其特征在于：该受控组播系统还包括有：与该组播路由器相连接的 portal 服务器和 AAA 服务器，其中 portal 服务器用作用户接入认证的接口，AAA 服务器用于保存用户加入组播组的权限配置，例如在 AAA 服务器上配置有每个用户有权加入的每个组播组的地址等；该组播路由器则配合 AAA 服务器一起共同完成对用户加入组播组的权限认证，并按照认证的结果下发控制命令，控制以太网交换机进行组播转发。

所述的组播路由器与 AAA 服务器之间采用对标准 radius 协议扩展了的华为公司的 radius+协议作为通信协议，而以太网交换机和组播路由器之间采用华为公司的华为组管理协议 HGMP（Huawei Group Management Protocol）作为控制协议。

本发明的受控组播的方法是这样实现的：该方法包括有下列步骤：首先进行接入认证处理，再由以太网交换机按端口划分vlan及对主机IGMP报文进行处

理，以及进行用户的识别、加入组播的认证及由路由器对IGMP报文进行处理，接着由组播路由器控制以太网交换机进行组播转发，两者之间采用HGMP协议作为受控组播的控制协议；之后，交换机对HGMP控制报文进行处理和进行组播流的转发；主机完成转发后，就退出组播组并作相应的处理。

该方法包括有下列步骤：

（1）首先进行接入认证处理：当一主机访问网络时，首先要通过portal服务器提供的接口输入包括有用户名和密码的认证信息，并由AAA服务器通过这些信息来认证该主机的身份；通过认证后，路由器将该主机的用户标识及其对应的vlan号记录在一个“用户组播访问权限表”中；

（2）以太网交换机按端口划分vlan及对主机IGMP报文进行处理：以太网交换机是根据端口划分vlan，每个端口划分为一个vlan，且其每个端口连接一个主机用户，当交换机收到主机发来的IGMP报文时，用该报文的目的MAC地址查找CAM表进行转发，其转发流程与单播报文相同：即若查到该目的MAC地址所对应的端口时，按查到的端口转发组播报文，若没有查到该目的MAC地址所对应的端口时，将组播报文转发到所有端口；

（3）进行用户的识别、加入组播的认证及路由器对IGMP报文进行处理：路由器收到IGMP Membership Report报文后，因为组播路由器收到的从以太网交换机发来的数据包都有vlan号，通过查找第（1）步骤中记录的“用户组播访问权限表”，可以知道对应用户的UserID，也就是知道该IGMP Membership Report报文是哪个用户发送的，然后以查到的UserID为用户名，以主机所要加入的组播地址为属性，发送扩展的radius认证报文到AAA服务器进行认证，由AAA服务器根据用户申请的业务决定是否让用户加入：如果用户拥有权限，则发送accept报文作回应，否则发送reject报文回应；路由器收到reject报文后不作任何处理，收到accept报文后将用户能够加入的组的组播地址写到“用户组播访问权限表”中，并对该主机加入的报文作通常组播路由器的例行处理，然后生成一个HGMP Join报文发送到交换机，该报文包含了申请加入组播组的主机所

连接的端口对应的vlan号和申请加入的组播地址，并且包含Join命令域；此外，组播路由器还要如同普通组播路由器一样地对IGMP Membership Report报文进行建立组播转发树的常规处理；

（4）由组播路由器控制以太网交换机进行组播转发，两者之间采用HGMP协议作为受控组播的控制协议：在以太网交换机上由组播路由器控制其组播转发表的生成与删除，当组播路由器允许某个主机加入某个组时，它给交换机发送包含有申请加入组播组的主机的vlan号和申请加入的组播地址的HGMP join报文；当组播路由器要终止某个主机加入某个组时，它给交换机发送包含有终止加入组播组的主机的vlan号和终止加入的组播组地址的HGMP leave报文，通过这种方法，组播路由器控制以太网交换机的的组播转发；

（5）交换机对HGMP控制报文进行处理：当交换机收到HGMP Join报文后，用组播地址对应的mac地址查CAM表，如果能够找到与其对应的一个表项，则通过报文中的vlanID查表来获得该主机端口号，然后将该端口号加入到该表项中；如果不能找到，则在CAM表中增加一个表项，该表项包含该组播地址所对应的mac地址、申请加入组播组的主机的端口号以及与交换机相连的路由器的端口号；当交换机收到HGMP Leave报文后，用组播地址对应的mac地址查CAM表而得到一个表项，再通过vlanID查表来获得该主机端口号，然后将该端口号从该表项中删除，如果该端口号是该表项的唯一一个端口，则删除整个表项；

（6）组播流的转发：当路由器收到组播源发来的组播流时，将该组播流按照转发表转发给出端口，路由器在处理主机的IGMP Membership Report报文时，不是按vlan号而是按交换机的实际端口建立组播转发出口，所以一个连接路由器的交换机在组播转发表中只有一个出口，组播流只发一份拷贝到交换机；

（7）主机退出组播组：当主机完成组播后，需要退出组播组时，由主机发送IGMP Leave报文要求退出组播组，路由器在收到该离开报文后，提取报文中的vlanID，并通过它查找第（1）步骤中建立的“用户组播访问权限表”得到对应的表项，删除该表项中成员离开报文所指示的组播地址，并完成通常路由器

对成员离开报文的例行处理，再生成一个HGMP Leave报文发给交换机，该报文包含了想要离开组播组的主机的vlan号和要离开的组播地址，并且包含Leave命令域。

所述的以太网交换机的组播转发表与单播转发表是共用的。

以太网交换机在转发报文时，若报文转发到组播路由器端口，使用 vlan 协议；否则，向别的端口发送报文时不用 vlan 协议。

上述第（6）步骤中的组播路由器发送给交换机的组播数据包不加 vlan 号，以避免为同一个交换机上的不同主机的每个 vlan 分别发送一份数据而浪费带宽的缺陷。

上述第（7）步骤中的主机退出组播组的操作还可以通过下述方法实现之：路由器在获知用户下线时主动发送 HGMP Leave 报文而停止向用户发送组播流，其具体实现方法与 IGMP Leave 报文的操作步骤相同。

该受控组播的实现方法还对组播发送者进行控制：当主机向某个组播组发送数据时，第一个接收该数据的组播路由器利用组播访问控制列表（Access Control List，简称：ACL）对数据报文进行过滤，只有满足其要求的报文才能被转发到组播树。

所述的组播访问控制列表 ACL 是由命令字、源地址和组地址（即：目的地址）构成。

所述的组播访问控制列表 ACL 是由一个集中的组播业务控制服务器来下发给各组播路由器，以便路由器藉由该组播访问控制列表 ACL 完成控制发送者的功能，该组播业务控制服务器同时兼作 AAA 服务器。

所述的组播访问控制列表 ACL 也可通过一个集中的策略服务器或网管下发，以消除分散配置引起的不便。

本发明的主要优点是：在用户加入组播组时，提供了认证授权的技术手段，确保只有授权用户才能进入该组播组；并且通过端口、用户和vlanID的一一对应关系，再加上对用户的接入认证，可以很方便地识别加入或离开组播组的用

户。组播路由器能够对二层交换机的组播转发功能执行带有决策性的主动控制，还可以将其控制策略下发到以太网交换机，较好地解决了对IP组播业务的受控问题。再者，在主机不发送IGMP Leave的情况下离开组播组（如组播应用程序异常终止）时，还可以通过用户下线主动停止用户的组成员身份。而且，在引入本发明的控制手段后，并没有影响其转发效率。所以，本发明具有很好的推广应用前景。

附图说明

图 1 是现在使用的 CGMP 报文格式示意图。

图 2 是现在使用的 CGMP 工作过程中主机 Host 1 第一个加入组播组 224.1.2.3 的信号流向示意图。

图 3 是现在使用的 CGMP 工作过程中主机 Host 4 第二个加入组播组 224.1.2.3 的信号流向示意图。

图 4 是本发明的受控组播系统的系统组成结构示意图。

图 5 是本发明的受控组播中主机 Host 1 进行接入认证时的信号流向示意图。

图 6 是本发明的受控组播中主机 Host 1 第一个加入组播组 224.1.2.3 的信号流向示意图

图 7 是本发明的受控组播中主机 Host 4 第二个加入组播组 224.1.2.3 的信号流向示意图。

图 8 是本发明的受控组播中路由器转发组播流的信号流向示意图。

图 9 是本发明的受控组播中主机 Host 1 离开组播组 224.1.2.3 的信号流向示意图。

图 10 是本发明的受控组播系统中的集中控制方案的示意图。

具体实施方式

参见图 4，本发明是一种受控组播的系统，包括有以太网交换机 1 和组播路由器 2，其中以太网交换机 1 下行连接各用户主机，上行与组播路由器 2 相连接，该组播路由器 2 上行连接其他系统的组播路由器 5，该以太网交换机 1 完成二层组播交换，该以太网交换机与用户主机之间使用 IGMP V2（版本 2）协议作为组管理协议；该受控组播系统还包括有：与该组播路由器 2 相连接的 portal 服务器 3 和 AAA 服务器 4，其中 portal 服务器 3 用作用户接入认证的接口，AAA 服务器 4 用于保存用户加入组播组的权限配置，组播路由器 2 与 AAA 服务器 4 之间为 Client-server 结构，该组播路由器 2 配合 AAA 服务器 4 一起共同完成对用户加入组播组的权限认证，并按照认证的结果下发控制命令，控制以太网交换机 1 进行组播转发。本发明的组播路由器 2 与 AAA 服务器 4 之间采用对标准 radius 协议扩展了的华为公司的 radius+协议作为通信协议，而以太网交换机 1 和组播路由器 2 之间采用华为公司的华为组管理协议 HGMP（Huawei Group Management Protocol）作为控制协议。

下面结合图 5－图 10 的各个附图和一个具体的实施例，详细描述本发明中主机加入组播组的全部过程的实现方法和操作步骤：

参见图 5，当某一主机（假设是 Host 1）要访问网络时，它首先要通过 portal 服务器提供的接口来进行接入的身份认证，AAA 服务器是认证服务器，图中 AAA 服务器中右侧方框中的 UserID 表示用户标识，即用户认证时输入的用户名，group 表示用户加入的组播组地址。以太网交换机（LAN switch）根据端口划分 vlan，每个端口接一个用户。其中端口 1 接组播路由器，端口 2－5 分别连接各主机用户 Host 1－Host 4。通过认证后，组播路由器记录了主机 host1 的用户标识（即：host1）及对应的 vlan 号：vlan 1（这里假设用户 Host 1 帐户中的用户名为 host1）。

参见图 6，当主机 Host 1 想加入组播组（假设是 224.1.2.3 组）时，它发送 IGMP Membership Report 报文加入组播组 224.1.2.3，交换引擎（Switching

Engine）用从该报文中的目的 mac 地址 0100.5e01.0203 查找 CAM 表，因为 CAM 表中没有匹配项，该报文被转发（flooding）到所有端口，包括 cpu 和路由器，其中转发到路由器的报文根据接收端口加上 vlan 号（对 host 1 就是 vlan1）。

路由器收到IGMP Membership Report报文后，提取报文中的vlanID: vlan 1，并通过它查表得到对应用户的UserID: host 1，然后以查到的UserID为用户名，以主机要加入的组播地址（224.1.2.3）为属性，发送扩展的radius认证报文到AAA服务器进行认证，AAA服务器根据用户申请的业务决定是否让用户加入。如果用户有权限，则发送accept报文作回应，否则发送reject报文回应。路由器收到reject报文后不作任何处理，收到accept报文后将用户能够加入的组的组播地址写到“用户组播访问权限表”中，对该主机加入报文作通常路由器的例行转发处理，然后生成一个HGMP Join报文发送到交换机，该报文包含了申请加入组播组的主机的vlan号: vlan 1和申请加入的组播地址: 224.1.2.3，并且包含Join命令域。

当交换机收到该HGMP Join报文后，在CAM表中加入一个表项，包含与该组播地址（224.1.2.3）对应的mac地址: 0100.5e01.0203，申请加入该组播组的主机的端口号: 2，以及与交换机相连的路由器的端口号: 1。其中，主机端口号是通过vlanID查表获得的。

参见图7，当又有新的主机（假设是第四个主机Host 4）加入组播组224.1.2.3时（假设其已通过接入认证，认证方法同上述第一步骤中的host1一样），同样发送IGMP Membership Report报文到交换机，交换引擎使用其目的mac地址0100.5e01.0203查寻CAM表，结果找到该表项，并将报文发送到该表项列出的端口1和2（即路由器和Host 1）。

路由器收到IGMP Membership Report报文后，提取该报文中的vlanID: vlan 4，并通过它查表得到对应用户的UserID: host 4，然后以查到的UserID为用户名，以主机要加入的组播地址（224.1.2.3）为属性，发送扩展的radius认证报文

到AAA服务器进行认证，AAA服务器根据用户申请的业务决定是否让用户加入。如果用户有权限，则发送accept报文作回应，否则发送reject报文回应。路由器收到reject报文后不作任何处理，收到accept报文后将用户能加入的组的组播地址写到“用户组播访问权限表”中，对该主机加入的报文作通常路由器的例行处理，然后生成一个HGMP Join报文发送到交换机，该报文包含了申请加入组播组的该主机的vlan号：vlan 4和申请加入的组播地址：224.1.2.3，并且包含Join命令域。

当交换机收到该HGMP Join报文后，用其组播地址（224.1.2.3）对应的mac地址（0100.5e01.0203）去查寻CAM表，由于在图6所述的步骤中第一个主机Host 1加入到224.1.2.3组之后，CAM表中已经存在一个表项，此次查询就能得到与上次相匹配的同一表项，通过vlanID查表获得该主机端口号：5，然后再将该端口号5加入到该表项中。

参见图8，当路由器收到组播源发来的组播流时，将组播流按转发表转发给出端口。因为路由器在处理主机的IGMP Membership Report报文时，并不是按vlan号而是按交换机的实际端口建立组播转发出口，所以一个连接路由器的交换机在组播转发表中只有一个出口，组播流只发一份COPY到交换机，组播数据包不加vlanID。

参见图9，当主机Host 1想要离开组播组224.1.2.3时，它发送IGMP Leave报文到交换机，在图9中与此时该主机Host 1发送的IGMP Leave报文相对应的是由Host 1引出的向上的箭头，交换引擎则使用其目的mac地址0100.5e01.0203查找CAM表，结果找到该表项，并将该报文发送到此表项列出的端口：1和5（即：路由器和Host 4）。

路由器收到其成员的离开报文后，提取该报文中的vlanID：vlan 1，并通过它查表得到对应的表项，删除该表项中成员离开报文所指示的组播地址224.1.2.3，即如图9所示，将其中路由器右侧方框中用户vlan 1所对应的用户有权加入的组播组地址group栏目的组播地址224.1.2.3删除之，再完成通常路由器

对成员离开报文的例行处理；然后生成一个HGMP Leave报文发给交换机（图9中与该HGMP Leave报文所对应的是由路由器引出的向下箭头），该报文包含了想要离开组播组的主机的vlan号：vlan 1和要离开的组播地址：224.1.2.3，并且包含Leave命令域。

当交换机收到该HGMP Leave报文后，用组播地址224.1.2.3对应的mac地址0100.5e01.0203查找CAM表得到一个表项，再通过vlanID查表获得发出IGMP Leave报文的主机的端口号：2，然后将该端口号2从该表项中删除。

以上各步骤是本发明受控组播的实现方法中对组播成员进行控制的具体操作步骤，此外，本发明的实现方法还对组播发送者执行相关控制，参见图 10。当主机（在图 10 中为信源 IDC）向某个组播组发送数据时，第一个接收该数据的组播路由器将首先通过组播业务控制服务器下载组播访问控制列表（Access Control List，简称：ACL），并利用该组播访问控制列表 ACL 对该数据报文进行过滤，只有满足通过要求的报文才能被转发到组播树。组播访问控制列表 ACL 是由命令字、源地址和组地址（也是目的地址）构成的。为了消除分散配置引起的不便，通常使用一个集中的组播业务控制服务器来完成向各组播路由器下发组播访问控制列表 ACL 而由这些组播路由器控制发送者的功能，同时，该组播业务控制服务器还兼作 AAA 服务器，当然也可以通过一个集中的策略服务器或网管下发组播访问控制列表。

本发明的组播系统及其实现方法已经在申请人研制的若干设备（例如：LANSWITCH系列交换机、QUIDWAY NetEngine系列路由器等设备）上进行了试验性实施，这些试验的结果是成功的，实现了要对组播实行控制的发明目的。

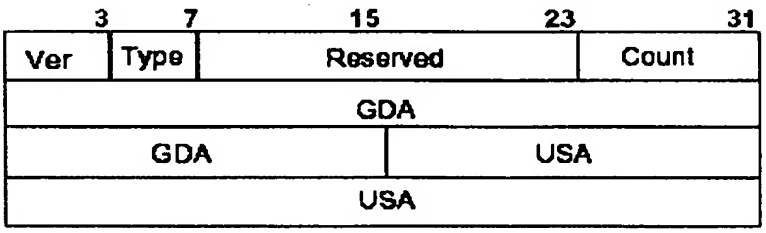

3
7
15
23
31
Ver
Type
Reserved
Count
GDA
GDA
USA
USA

图 1

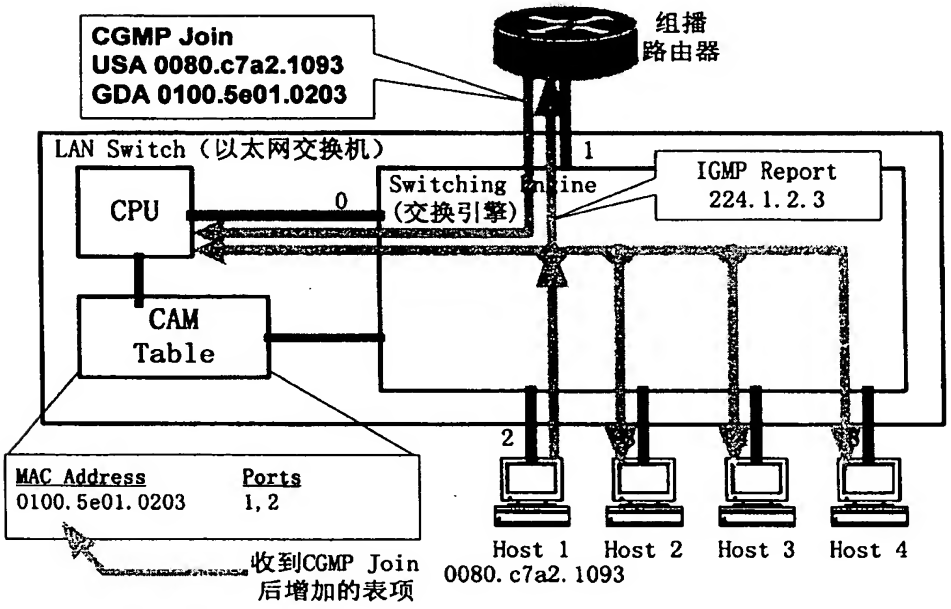

CGMP Join
USA 0080.c7a2.1093
GDA 0100.5e01.0203
组播
路由器
LAN Switch（以太网交换机）
1
CPU
0
Switching Engine
(交换引擎)
IGMP Report
224.1.2.3
CAM
Table
2
MAC Address
Ports
0100.5e01.0203
1,2
收到CGMP Join
后增加的表项
Host 1
Host 2
Host 3
Host 4
0080.c7a2.1093

图 2

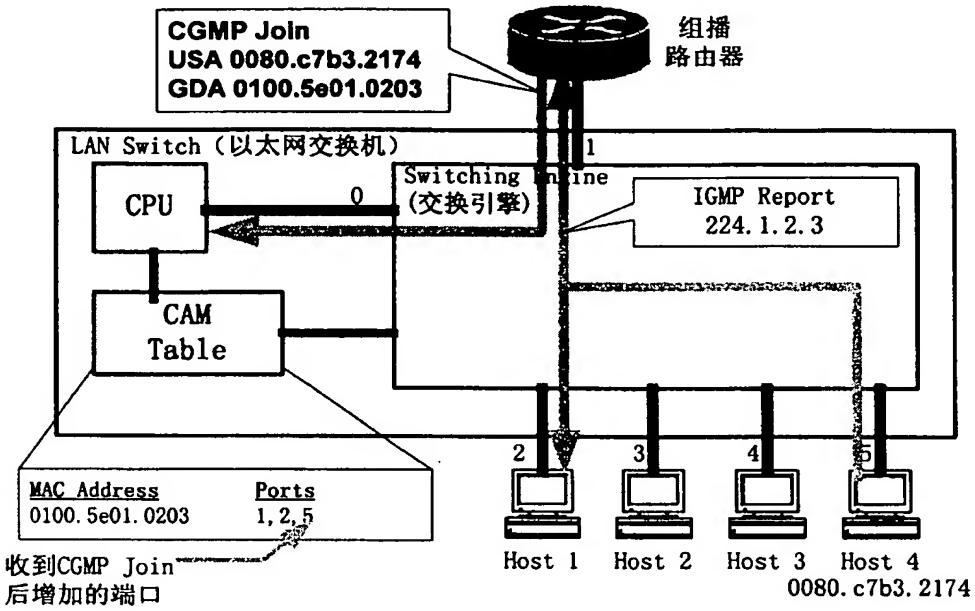

CGMP Join
USA 0080.c7b3.2174
GDA 0100.5e01.0203
组播
路由器
LAN Switch（以太网交换机）
CPU
0
1
Switching Engine
(交换引擎)
IGMP Report
224.1.2.3
CAM
Table
2
3
4
5
MAC Address
Ports
0100.5e01.0203
1,2,5
收到CGMP Join
后增加的端口
Host 1
Host 2
Host 3
Host 4
0080.c7b3.2174

图 3

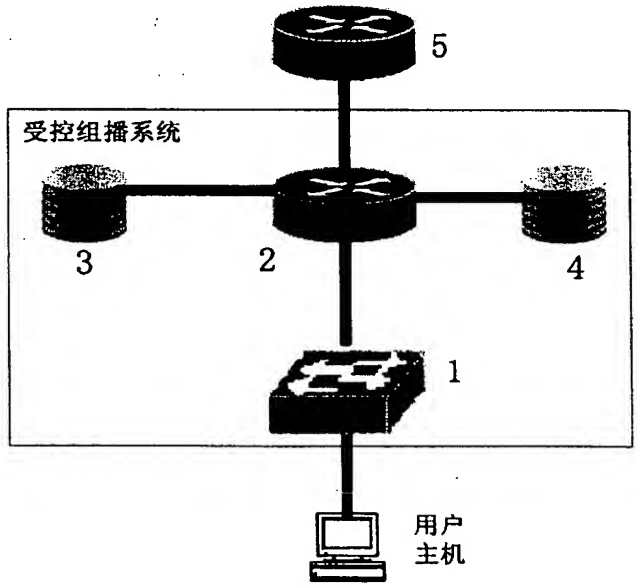

5
受控组播系统
3
2
4
1
用户
主机

图 4

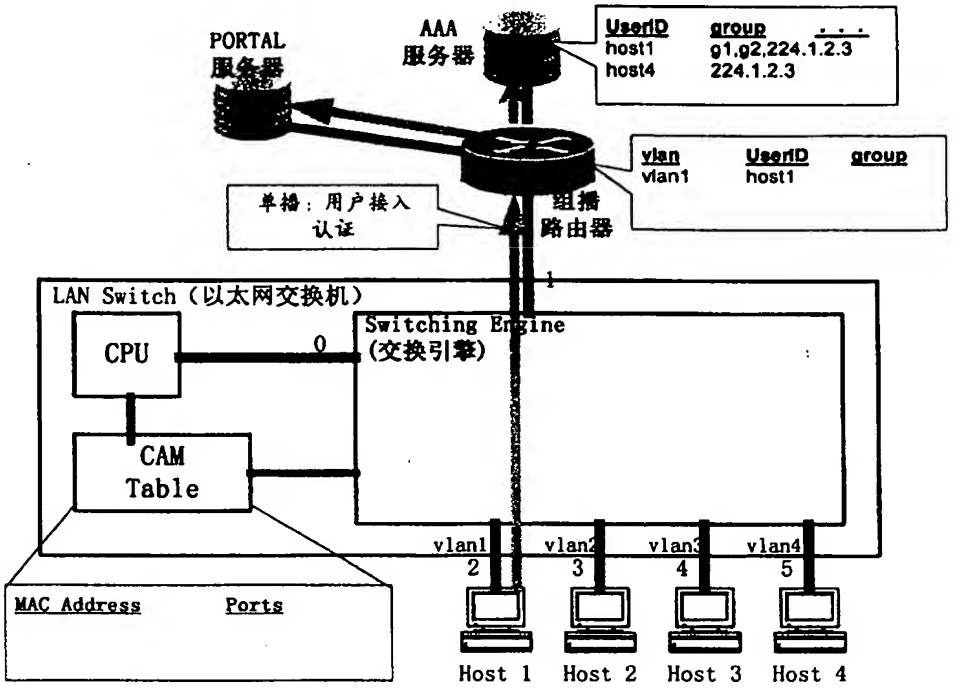

PORTAL
服务器
AAA
服务器
UserID group
host1 g1,g2,224.1.2.3
host4 224.1.2.3
vlan UserID group
vlan1 host1
单播：用户接入
认证
组播
路由器
LAN Switch（以太网交换机）
CPU
0
Switching Engine
(交换引擎)
CAM
Table
1
vlan1 vlan2 vlan3 vlan4
2 3 4 5
MAC Address Ports
Host 1 Host 2 Host 3 Host 4

图 5

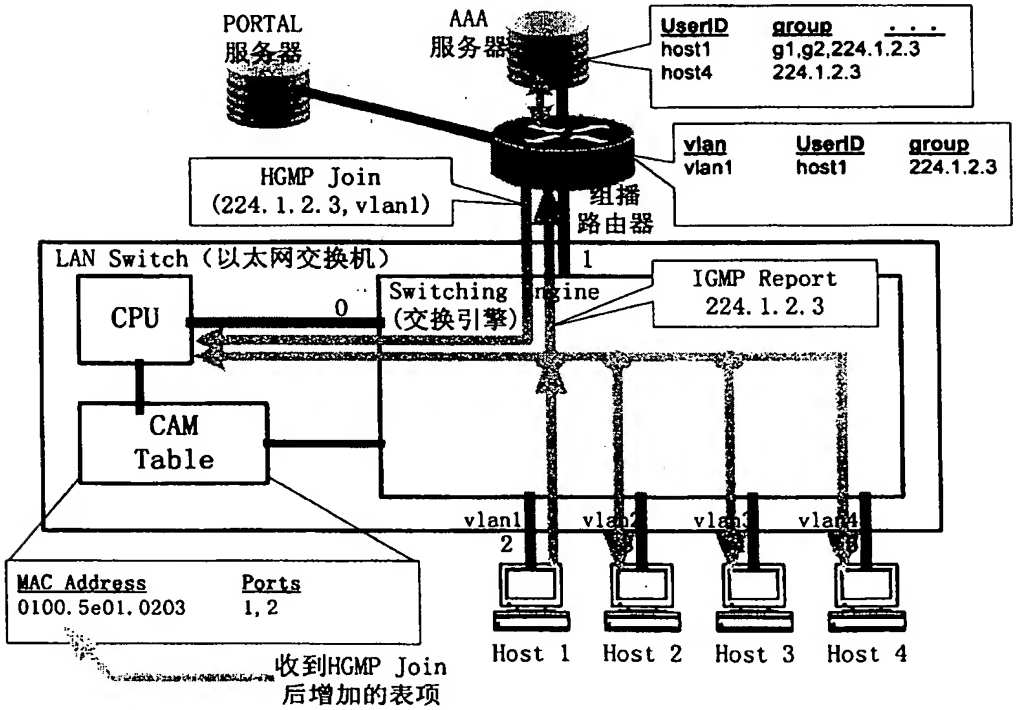

PORTAL
服务器
AAA
服务器
UserID group
host1 g1,g2,224.1.2.3
host4 224.1.2.3
vlan UserID group
vlan1 host1 224.1.2.3
HGMP Join
(224.1.2.3, vlan1)
组播
路由器
LAN Switch（以太网交换机）
1
CPU
0
Switching Engine
(交换引擎)
IGMP Report
224.1.2.3
CAM
Table
vlan1
2
MAC Address Ports
0100.5e01.0203 1,2
收到HGMP Join
后增加的表项
Host 1 Host 2 Host 3 Host 4

图 6

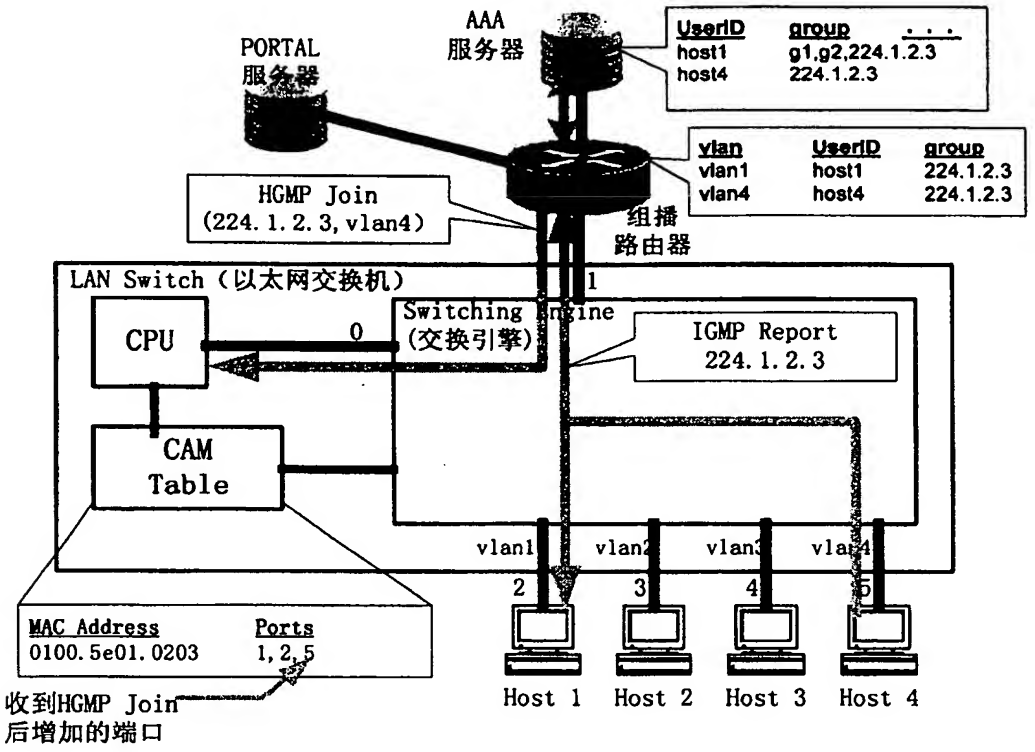

AAA
服务器
PORTAL
服务器
UserID group . . .
host1 g1,g2,224.1.2.3
host4 224.1.2.3
vlan UserID group
vlan1 host1 224.1.2.3
vlan4 host4 224.1.2.3
HGMP Join
(224.1.2.3, vlan4)
组播
路由器
LAN Switch (以太网交换机)
1
CPU
0
Switching Engine
(交换引擎)
IGMP Report
224.1.2.3
CAM
Table
vlan1
vlan2
vlan3
vlan4
2
3
4
5
MAC Address Ports
0100.5e01.0203 1,2,5
收到HGMP Join
后增加的端口
Host 1
Host 2
Host 3
Host 4

图 7

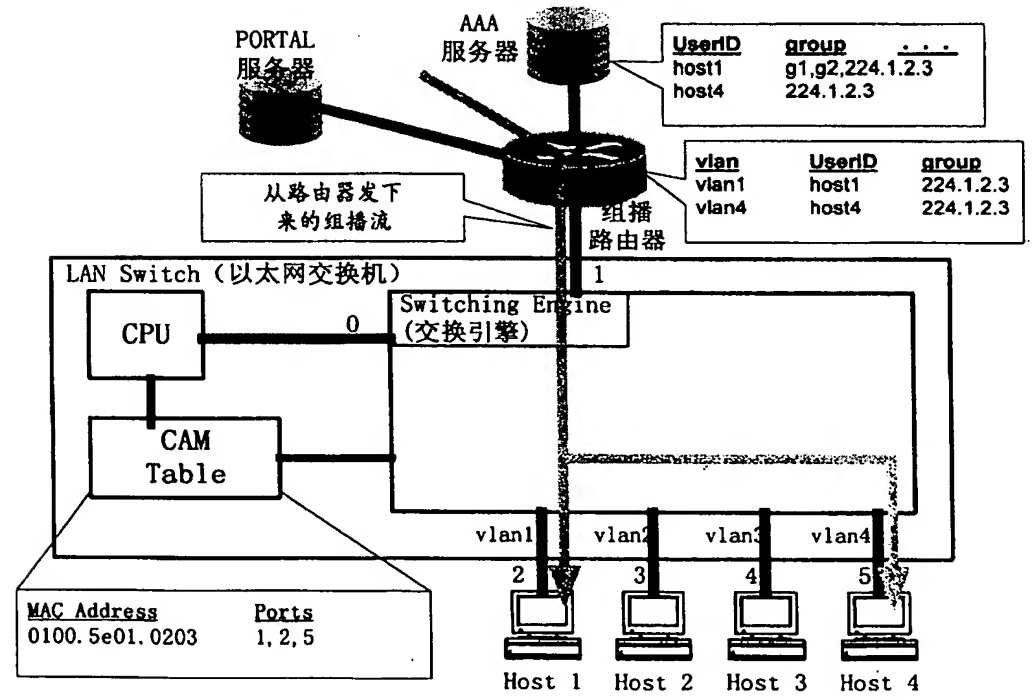

AAA
服务器
PORTAL
服务器
UserID group . . .
host1 g1,g2,224.1.2.3
host4 224.1.2.3
vlan UserID group
vlan1 host1 224.1.2.3
vlan4 host4 224.1.2.3
从路由器发下
来的组播流
组播
路由器
LAN Switch (以太网交换机)
1
CPU
0
Switching Engine
(交换引擎)
CAM
Table
vlan1
vlan2
vlan3
vlan4
2
3
4
5
MAC Address Ports
0100.5e01.0203 1,2,5
Host 1
Host 2
Host 3
Host 4

图 8

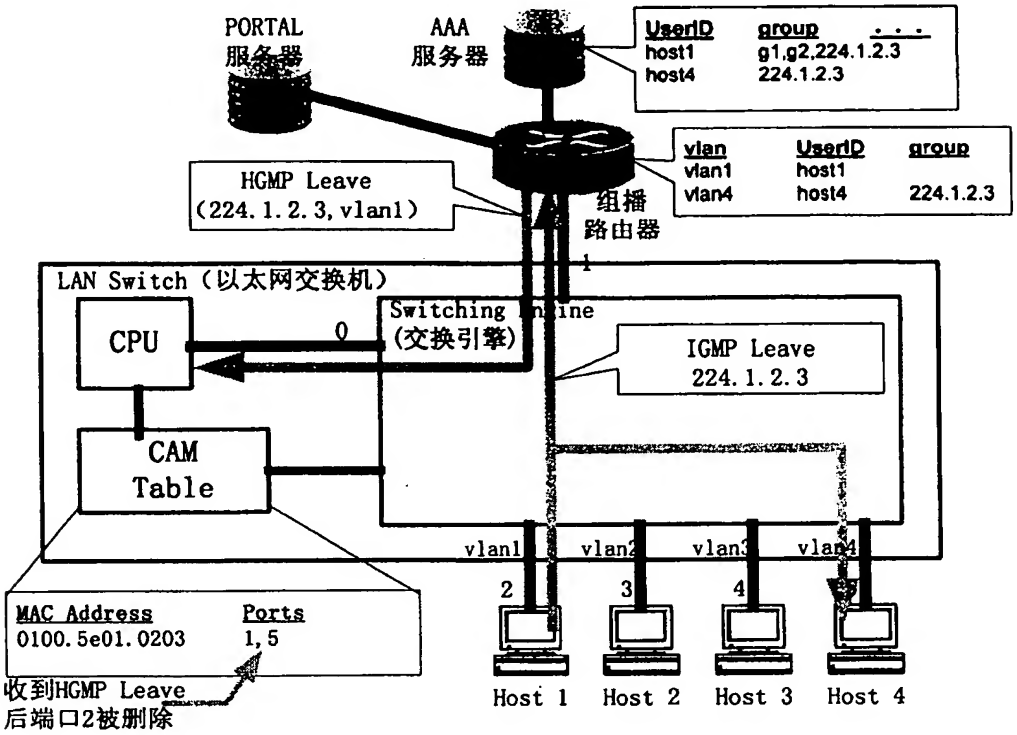

PORTAL
服务器
AAA
服务器
UserID group
host1 g1,g2,224.1.2.3
host4 224.1.2.3
vlan UserID group
vlan1 host1
vlan4 host4 224.1.2.3
HGMP Leave
(224.1.2.3, vlan1)
组播
路由器
LAN Switch (以太网交换机)
CPU
Switching Engine
(交换引擎)
IGMP Leave
224.1.2.3
CAM
Table
vlan1
vlan2
vlan3
vlan4
2
3
4
MAC Address Ports
0100.5e01.0203 1,5
收到HGMP Leave
后端口2被删除
Host 1
Host 2
Host 3
Host 4

图 9

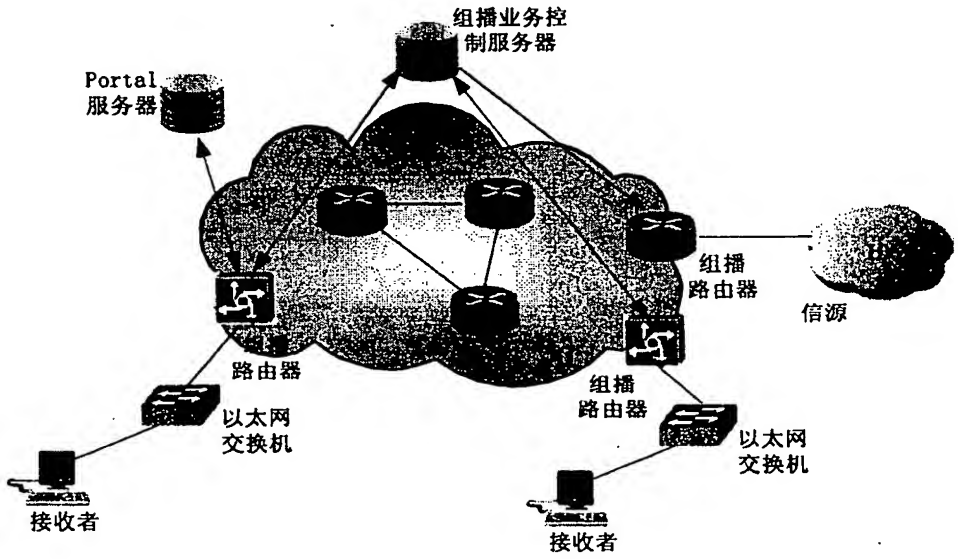

组播业务控
制服务器
Portal
服务器
组播
路由器
信源
路由器
以太网
交换机
组播
路由器
以太网
交换机
接收者
接收者

图 10